Privacy Impact Assessment
for the

Joint Integrity Case Management System (JICMS)

DHS/CBP/PIA-044

July 18, 2017

Contact Point
Jessica R. Samuel
Investigative Operations Division
Office of Professional Responsibility
U.S. Customs and Border Protection
(202) 344-3374

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) created the Joint Integrity Case Management System (JICMS) to record claims of employee misconduct, manage criminal and administrative investigations, and to track employee and contractor disciplinary actions. The CBP Office of Professional Responsibility (OPR) and U.S. Immigration and Customs Enforcement (ICE) OPR are responsible for the overall operation of JICMS, however other DHS components may use JICMS for their internal affairs case management. CBP is conducting this Privacy Impact Assessment (PIA) to assess the privacy risks and mitigations associated with JICMS because it collects, stores, and uses personally identifiable information (PII) about DHS employees, contractors, and members of the public.

Overview

The U.S. Customs and Border Protection (CBP) Office of Professional Responsibility (OPR) is responsible for ensuring compliance with all CBP-wide programs and policies relating to corruption, misconduct, or mismanagement and for executing the internal security, integrity, and management inspections programs. Through the national headquarters in Washington, D.C., and strategically located regional field offices, OPR screens potential CBP employees for suitability; educates employees concerning ethical standards and integrity responsibilities; conducts inquiries into employee misconduct allegations; evaluates physical security threats to CBP employees, facilities, and sensitive information; and inspects CBP operations and processes for managerial effectiveness and improvements. The OPR mission is clear and critically important - to promote the integrity and security of the CBP workforce.

The OPR Investigative Operations Division (IOD) is responsible for conducting investigations of alleged criminal and serious, non-criminal misconduct on the part of CBP employees. IOD is comprised of Special Agents assigned to CBP headquarters and over twenty field offices. OPR field offices are managed by Special Agents in Charge and Resident Agents in Charge located strategically throughout the United States where the threat of internal corruption is most pervasive. IOD coordinates its internal investigative activity with the Office of Inspector General (OIG), U.S. Immigration and Customs Enforcement (ICE) OPR, the U.S. Department of Justice Federal Bureau of Investigation (FBI), and numerous other federal, state, and local law enforcement authorities. IOD Special Agents participate on a full-time basis as members of numerous Border Corruption and Public Corruption Task Forces.

IOD also manages the Joint Intake Center (JIC), which serves as the central "clearinghouse" for receiving, processing, and tracking allegations of misconduct involving personnel and contractors employed by CBP and ICE. The JIC provides CBP and ICE with a centralized and uniform system for processing reports of alleged misconduct. All reports of

misconduct are coordinated with the DHS OIG and referred to the appropriate office for investigation, fact-finding, or immediate management action.

The Joint Integrity Case Management System (JICMS) is a case management system, originally used only by CBP and ICE at the JIC, but has now expanded to users within CBP, ICE, the National Protection and Programs Directorate (NPPD), and DHS Headquarters (HQ). JICMS provides DHS components with the capability to record employee and contractor misconduct, to conduct criminal and administrative investigations, and to track employee and contractor disciplinary actions. JICMS also collects information about members of the public whose information is relevant to the investigation of the alleged misconduct or complaint, including: complainants, witnesses, alleged perpetrators, or any other persons identified as relevant to the investigation. JICMS is managed by CBP OPR and ICE OPR, but used by 1) CBP Labor and Employee Relations (LER), 2) ICE Employee Labor Relations (ELR), 3) DHS OIG, 4) NPPD, and 5) DHS Office of the Chief Security Officer (OCSO).

Roles and Responsibilities of DHS OIG, Offices, and Employees

Within DHS, OIG and component Offices of Professional Responsibility (or Internal Affairs) have shared investigatory authorities for employee misconduct and internal investigations. OIG, while organizationally a part of DHS, operates independent of DHS and all offices within it. OIG is authorized, among other things, to initiate, conduct, supervise, and coordinate audits, investigations, inspections, and other reviews relating to the programs and operations of DHS; and receive and investigate complaints or information from employees, contractors, and other individuals concerning the possible existence of criminal or other misconduct constituting a violation of law, rules, or regulations, a cause for suspension or debarment, mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety.

Pursuant to DHS policy,[1] component OPRs are required to promptly advise OIG of allegations of specific types of misconduct,[2] and when they become aware of any audit, inspection, or investigative work being performed or contemplated within their offices by or on behalf of an OIG from outside DHS, the Government Accountability Office, or any other law enforcement authority, unless restricted by law.

Referral to OIG

The categories of misconduct identified below must be referred to OIG immediately upon receipt of the allegation.[3] The following allegations must be referred to OIG:

[1] Department of Homeland Security Management Directive System MD Number 0810.1 (6/10/2004), *The Office of Inspector General*.
[2] Identified in Appendix A of DHS MD 0810.1.
[3] No investigation shall be conducted by the component internal affairs offices prior to referral to OIG unless failure to do so would pose an imminent threat to human life, health, or safety, or result in the irretrievable loss or

- Criminal misconduct by any DHS employee;
- Any type of misconduct (criminal, civil, or administrative) by employees at the Grade 15 level or higher;
- Serious, noncriminal misconduct by a law enforcement officer ("serious, noncriminal misconduct" is conduct that, if proved, would constitute perjury or material dishonesty, warrant suspension as discipline for a first offense, or result in loss of law enforcement authority. For purposes of this policy, a "law enforcement officer" is defined as any individual who is authorized to carry a weapon, make arrests, or conduct searches);
- Discharged firearm that results in death, personal injury, or warrants referral to the Civil Rights Criminal Division of the Department of Justice;
- Fraud by contractors, grantees, or other individuals or entities receiving DHS funds or engaged in the operation of DHS programs or operations; and
- Visa fraud by DHS employees working in the visa issuance process.

In addition, OIG reserves the right to investigate allegations against individuals or entities that do not fit into the categories cited if the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling, serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

With regard to categories not cited for referral, the Organizational Elements (OE)[4] offices initiate the investigation upon receipt of the allegation and notify OIG within five business days. OIG notifies the OE offices if it intends to assume control or become involved in the investigation. Absent such notification, the OE office shall maintain full responsibility for these investigations. In addition, OIG refers any allegation it receives to the appropriate OE office within five business days if OIG determines not to investigate the allegation.

OE offices provide monthly reports to OIG on all open investigations. In addition, upon request, the OE offices shall provide OIG with a complete copy of the Report of Investigation (ROI),[5] including all exhibits, at the completion of the investigation. Similarly, OIG shall provide the OE offices, upon request, with a complete copy of any ROI relating to its OE, including all

destruction of critical evidence or witness testimony.

[4] Organizational Elements (OE) are offices within DHS that are responsible for: internal affairs, inspections, audits, or Professional Responsibility. More information about OEs can be found later in this document.

[5] The Report of Investigation (ROI) is the final closing report and any accompanying exhibits. Once OPR's investigation is completed, OIG can request a copy of the final ROI. If OIG accepted an allegation of employee misconduct for investigation, OIG will provide a copy of the final OIG ROI to OPR upon completion of the investigation. At any time during an OPR investigation, OIG can request an update of the ongoing investigative activities and choose to take over the case for investigation.

exhibits, at the completion of the investigation. OIG may request more frequent or detailed reports on any investigations at any time.

With regard to categories not specified above, the OE offices will initiate the investigation upon receipt of the allegation, and shall notify within five business days the OIG's Office of Investigations of such allegations. OIG shall notify the OE offices if OIG intends to assume control over or become involved in such an investigation, but absent such notification, the OE office shall maintain full responsibility for these investigations.

Any allegations received by OIG that do not come within the categories specified above, or that OIG determines not to investigate, will be referred within five business days of receipt of the allegation by OIG to the appropriate OE office along with any confidentiality protections deemed necessary by OIG. OIG shall have the right to request more frequent or detailed reports on any investigations and to reassert at any time exclusive authority or other involvement over any matter within its jurisdiction.

DHS OIG

The DHS OIG uses JICMS to review initial allegations to determine whether to exercise its right to conduct an investigation. OIG reports directly to the Secretary of Homeland Security and has the authority to initiate, conduct, supervise, and coordinate audits, investigations, inspections, and other reviews related to programs and operations within DHS, including criminal and misconduct allegations reported by employees, contractors, and other individuals. This authority gives OIG first right of refusal to investigate all reported allegations reported within JICMS.

DHS Organizational Elements

Organizational Elements (OE) are offices within DHS that are responsible for: internal affairs, inspections, audits, or Professional Responsibility. These OE offices are responsible for the following:

1. Informing OIG of all allegations of misconduct and any audit, inspection, or investigation being performed or contemplated within their offices by or on behalf of non-DHS OIGs, the Government Accountability Office, or any other law enforcement authority, unless restricted by law;
2. Providing OIG personnel with adequate and appropriate office space, equipment, computer support services, temporary clerical support, and other services to effectively accomplish their mission when requested;
3. Providing OIG personnel with access to any files, records, reports, or other information that may be requested either orally or in writing;

4. Disseminating OIG policies within their component; components retain the option of implementing further instructions as necessary to implement OIG policy;
5. Providing OIG personnel with access to DHS staff and other appropriate persons; and
6. Identifying classified or sensitive information to OIG to ensure proper handling.

DHS Employees

All DHS employees are responsible for reporting suspicions of legal or regulatory violations to OIG, or the appropriate DHS component office of internal affairs, professional responsibility, or security. All DHS employees must:

1. Disclose complete and accurate information about matters under investigation or review;
2. Inform the investigating entity (either OIG or the internal affairs offices within a DHS component) of any issues requiring attention;
3. Not conceal information or obstruct audits, inspections, investigations, or other official inquiries;
4. Know they are subject to criminal prosecution and disciplinary action, including removal, for knowingly and willfully furnishing false or misleading information to investigating officials; and
5. Know they are subject to disciplinary action for refusing to provide documents, information, answers to questions, or signed sworn statements requested by OIG, unless an employee is the subject of an investigation that can lead to criminal prosecution.

Reporting and Investigation Process

A case is initiated when an individual sends an allegation via email, fax, general mail, or telephone to the JIC, OPR, or an equivalent internal investigation field office regarding an employee or contractor. Upon receipt of an allegation, it is entered into JICMS. Once entered into JICMS, the allegation: 1) receives a preliminary classification based on the nature and severity of the allegation; 2) is reviewed by OIG to determine if it wants to take ownership of the case (OIG has first right of refusal); 3) if OIG does not take ownership of the case, it is routed to specific program areas for review and investigation; 4) is investigated to determine the validity of the alleged violation of a law, rule, or regulation; and 5) is documented according to the investigation, findings, and follow-up actions.

There are several routes the case can take depending on the type and seriousness of the allegation: 1) if an allegation involves a serious violation and requires validation, an investigation can be conducted by component investigators or OIG; 2) less serious allegations can be assigned to a designated component fact finder, who performs an administrative inquiry; or 3) depending on the facts of the case, local management may take immediate action or dismiss the allegation.

Component employee relations offices receive and review the investigations reports, administrative inquiries, and management inquiries. Generally, these offices coordinate the administration of adverse actions, and other forms of discipline for substantiated violations by their employees and then, record decisions and dispositions of the disciplinary process in JICMS. CBP LER and ICE ELR also document the decision and disposition of the disciplinary process in CBP's Human Resources Business Engine (HRBE),[6] a human resources system.

Types of Allegations Reported

Allegations reported to the JIC are intended for activities involving substantive misconduct or serious mismanagement. An example of this type of misconduct would include criminal activities that violate state or federal criminal laws including the arrest of an employee. Other examples of reportable misconduct would include: actions that could jeopardize the mission, misuse of official position or information, falsification (of documents, work products, reports, etc.), workplace violence or harassment, improper association (*e.g.*, with individual(s) who are suspected or known to be connected to criminal activities), or willful misuse of government property.

Less serious types of conduct or performance issues should be reported directly to management. Examples of these types of issues would include: leave or tardiness issues, job performance issues, violation of the dress code, personality conflicts, rudeness and disruptive behavior, passenger or citizen complaints, or improper use of government credit cards of $500 or less and delinquent payment of these credit cards of $1,000 or less. However, if a less serious issue is reported to the JIC, it is documented in JICMS, given a minor allegation classification, and referred to the appropriate office for action.

Disciplinary Actions

Disciplinary action procedures may vary among the components. However, in general, component employee relations offices coordinate the administration of: adverse actions, discipline, and letters of reprimand for violations by employees. Employee relations staff receive the results of investigations and management inquiry reports. Then, staff in coordination with counsel: 1) screen cases for potential adverse action; 2) remand those cases not meeting standards to local management; 3) convene the component discipline or adverse action board to evaluate cases and propose action, as appropriate; and 4) coordinate due process activities. Due process activities consist of: issuing/providing notice of the proposed action in writing to the subject, granting the subject the opportunity to reply to the proposal, and determining the appropriate disciplinary action.

[6] *See* DHS/CBP/PIA-032 Human Resources Business Engine (HRBE) (July 26, 2016), *available at* https://www.dhs.gov/privacy.

Risks Associated with JICMS

Given the serious nature of many allegations recorded in JICMS, it is critical that JICMS users have accurate and timely information to make investigatory and disciplinary decisions. Information within JICMS must also be properly secured and safeguarded from unauthorized access. Lastly, due to serious nature of the allegations and investigations within JICMS and the possibility for employee removal or discipline, JICMS must have strong access and redress procedures to the extent permissible by law. These risk are described in full below.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Subtitle B, Section 811 of the Homeland Security Act of 2002 gives the DHS Inspector General oversight responsibility for internal investigations performed by CBP Internal Affairs (renamed OPR). Department of Homeland Security Management Directive System MD Number 0810.1 establishes the purpose, responsibilities, policies, and procedures of all component offices of internal affairs, inspections, audits, or professional responsibility within DHS. In addition, it identifies general allegation categories covered by these offices.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

SORN coverage for JICMS is provided by DHS Internal Affairs SORN[7] and the associated Final Rule.[8]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The most recent Authority to Operate (ATO) was granted to the JICMS system on June 6, 2013. A reauthorization is pending publication of this Privacy Impact Assessment (PIA).

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, JICMS is covered by NARA record retention schedule N1-567-11-9. Information collected during inquiries or investigations is deleted or destroyed after twenty-five (25) years or one (1) year after the subject separates from DHS, whichever is later.

[7] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014).
[8] *See* Final Rule for Privacy Act Exemptions, 74 FR 42575 (August 24, 2009).

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

JICMS does not collect standardized information directly from members of the public and therefore, is not subject to the requirements of the Paperwork Reduction Act. However, members of the public may report allegations concerning DHS employees through the CBP Information Center.[9] The CBP Information Center then refers allegations of employee or contractor misconduct to the JIC. Members of the public may also submit information directly to the JIC via the JIC Hotline, fax, or mail. The information collected from individuals through the CBP Information Center is covered by OMB Number 1651-0136.

Individuals may also report allegations of misconduct through the DHS OIG Hotline.[10] The public-facing DHS OIG Hotline website and forms are exempt from the Paperwork Reduction Act pursuant to the Inspector General Empowerment Act of 2016.[11]

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The types of information entered into JICMS include: (1) information relating to an allegation received by the JIC, type of allegation received, and the nature of the allegation made; (2) tracking information regarding the status of investigation; and (3) ROI and related documentation, which may be subsequently reviewed as part of a criminal, administrative, or civil action or related matter; background investigations; or security clearances.

Information is collected and maintained about the following categories of individuals and types of records:

1. ***Subjects of Investigation***

The following information facilitates the recording and tracking of information from receipt of an allegation, through the investigative process, and finally, to disposition/discipline. These data elements also enable easy retrieval of information used in reporting and analysis. Social Security numbers may also be used to uniquely identify the subjects, sources, and witnesses of

[9] For information about how CBP collects allegation/complaint reports on CBP employees from members of the public, please *see* DHS/CBP/PIA-035 CBP Compliant Management System (CMS) (September 14, 2016), *available at* https://www.dhs.gov/privacy.
[10] *See* https://www.oig.dhs.gov/hotline.
[11] Pub. L. 114-317.

investigations, which are documented in JICMS. This is a list of the possible information collected and will vary from case to case.

- Subject Last Name
- Subject First Name
- Subject Type (position title, *e.g.*, Border Patrol Agent, CBP Officer, Port Director)
- Subject Office
- Source Code
- Allegation Code
- Social Security number (SSN) (not required but may be provided voluntarily from sources or members of the public, or may be accessible in source records)
- Series, Grade, Position Title
- Work Location
- Date of Birth (DOB)
- Other Disciplinary Actions
- Arrest Date
- Incident Date
- Reported Date
- Incident Location
- State Driver's License Number
- Vehicle Identification
- Vehicle License Plate
- Birth Certificate
- Alien Number
- Financial Information
- Civil and Criminal History Information
- Photographic Facial Image
- Other Disciplinary Actions

2. Complainants, Witnesses, and Individuals Associated with a Case

JICMS collects, uses, and maintains the following information for general contact and investigative purposes (data elements vary by case and complaint, not all of this information is included for each case):

- Name
- Mailing Address
- Telephone Number
- Facsimile Number
- Email Address
- Alien Number
- Social Security number (not required but may be provided voluntarily from sources or members of the public, or may be accessible in source records)
- Immigration Status
- Date of Birth
- Country of Citizenship

3. Employees and Contractors

JICMS collects, uses, disseminates, or maintains information on component employees and contractors, along with members of the public who are associated with a case. This category also includes information on the case agent, case officer, case supervisor, and employee relations staff. This information includes:

- Name
- Aliases
- Gender
- Series, Grade, Position Title
- Work Location
- Email Address
- Phone Number
- Home Address

4. Supporting Documents Related to Case

Primary case-related information maintained includes: Case Number, Case Type, Case Status, Case Notes, Case History, ROIs, Administrative Inquiry Reports (AIR), Disciplinary Actions, Case Opened/Case Closed Dates, and Case Summary.

2.2 What are the sources of the information and how is the information collected for the project?

Information is collected from individuals filing allegations of criminal or administrative violations, including, but not limited to individuals alleged to have been involved in such violations; individuals identified as having been adversely affected by matters being investigated; individuals who have been identified as associated with the investigation; and informants. These may be DHS employees, contractors, or members of the public.

Information is collected by CBP and ICE investigators, contractors, and fact finders[12] investigating the allegation. Additionally, DHS, CBP, and ICE plan to include social media sources for investigative purposes.[13]

Information is collected to verify and confirm investigative leads through third parties. Such sources may include eyewitnesses; third parties with financial or other information relating to the subject of the investigation, or the matters under investigation; other law enforcement agency personnel; and any other persons or entities with information pertinent to the matter under review. Information also may be extracted from U.S. Department of Agriculture (USDA) payroll and personnel records[14] and HRBE.[15] Investigators may also use information obtained from TECS,[16] National Crime Information Center (NCIC),[17] National Law Enforcement Telecommunications

[12] Designated agency fact finders are assigned to an OPR point of contact in order to work cases identified as administrative inquires. The fact finder and point of contact conduct a review of relevant facts and in gathering evidence, which includes taking of sworn statements from witnesses and subjects. The point of contact loads the evidence (exhibits) and closing report (the AIR) into JICMS.

[13] Initial complaints may include information, including screen prints, from social media. In addition, investigators may use social media information throughout the course of an investigation. Investigators document the use of social media information in the report of investigation.

[14] The SAP Business Warehouse provides JICMS with updated information for the entire CBP federal employee population every two weeks via an interface. The information is initially obtained by the CBP Mainframe via a direct link with the U.S. Department of Agriculture (USDA) National Finance Center (NFC) Mainframe. The data is transmitted once every two weeks in conjunction with the CBP payroll process. The SAP Business Warehouse sends the data via a direct feed to JICMS. JICMS uses this data to create and update employee biographic information in the system.

[15] DHS/CBP/PIA-032 Human Resources Business Engine (HRBE) (July 2016), *available at* https://www.dhs.gov/privacy.

[16] DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (December 22, 2010), *available at* https://www.dhs.gov/privacy.

[17] The National Crime Information Center (NCIC) is an FBI-owned system that assists law enforcement in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists. Additional information on NCIC is available at https://www.fbi.gov/services/cjis/ncic.

System (NLETS),[18] California Law Enforcement Telecommunication System (CLETS),[19] and commercial sources; however, this information is uploaded manually and there is no direct system interface between JICMS and TECS or its subsystems. If the case warrants, hard copies of TECS/NLETS information may be included in the JICMS file as an attachment. All data fields from HRBE are noted in Appendix A.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes, JICMS contains information from commercial sources and publicly available data sources when deemed appropriate. Commercial sources include subscriptions to law enforcement databases, such as Lexis Nexis and CLEAR. Such sources enable corroboration and verification of facts collected from individuals.

Commercial data is sometimes collected as background information: to verify addresses, identities, and contact information; to identify illegal activities; to identify possible witnesses; and for other investigative purposes.

JICMS will also contain information collected from publicly available social media sources, pending the completion of this PIA and approval of a Social Media Operational Use Template (SMOUT) by the DHS Privacy Office.

2.4 Discuss how accuracy of the data is ensured.

JICMS does not perform data quality tests to verify the accuracy of information maintained. However, accuracy verification is conducted at each level of the case. Case agents, officers, and supervisors perform separate checks to verify accuracy, completeness, and propriety of information entered in JICMS. Additionally, supervisory reviews of information in JICMS are performed as part of the ROI or AIR review process. Also, data is independently analyzed by headquarters investigative personnel when queried for routine and non-routine reporting requirements. Substantiated offenses forwarded to employee relations offices for the disciplinary process also are reviewed for accuracy and completeness.

---

[18] The National Law Enforcement Telecommunications System (NLETS) is a non-profit organization owned by the states that allows state and federal law enforcement agencies, as well as select international agencies, to securely share law enforcement, criminal justice, and public safety related information. Additional information on NLETS is available at http://www.nlets.org/.

[19] The California Law Enforcement Telecommunication System (CLETS) is a high-speed message switching system which became operational in 1970. CLETS provides law enforcement and criminal justice agencies access to various databases and the ability to transmit and receive point-to-point administrative messages to other agencies within California or via NLETS to other states and Canada. Broadcast messages can be transmitted intrastate to participating agencies and to regions nationwide via NLETS. CLETS has direct interface with the FBI's NCIC, NLETS, Department of Motor Vehicles (DMV), Oregon, and Nevada.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of over-collection, because JICMS receives a bi-weekly feed of all CBP employee personnel information from the USDA NFC, regardless of whether the employee is complainant, subject, or witness to an investigation.

Mitigation: This risk is not mitigated. CBP needs information to identify employees associated with a complaint, whether that employee is a subject, source, or witness. The complete feed enables CBP OPR to quickly and easily confirm the identity of employees without needing to confirm with other offices. However, because the majority of CBP employees are not likely to be implicated in any way in an investigation, this constitutes an over-collection that cannot be fully mitigated.

Privacy Risk: Due to the law enforcement and investigatory nature of records maintained within JICMS, there is a risk that information in JICMS may not always be accurate or timely.

Mitigation: This risk is not fully mitigated within JICMS. However, accuracy verification is conducted at each level of the case. Investigators are trained to conduct a complete investigation to ensure that sufficient and relevant information is collected to resolve the issue in an unbiased manner. Sources are documented in detail to assess reliability of the information and substantiated through other sources when available. Managerial reviews are conducted on a regular basis to ensure accurate interpretation and logical presentation of the information, and adherence to applicable laws and regulations, as well as policies and procedures governing the rights and privacy of those involved in the investigation.

Privacy Risk: There is a risk to transparency, individual participation, and data integrity because much of the information stored within JICMS is not collected directly from the subject of the allegation.

Mitigation: This risk cannot be fully mitigated. Given the nature of internal investigations, information initially may not be collected from the subject of the investigation because notice of the investigation may result in disclosure of investigative procedures and evidence. However, information is collected directly from the individual who reports the allegation or complaint, and is then entered into JICMS by DHS employees. This entry initiates the investigative process. Then, information is collected from sources other than the individual to verify and confirm information. Such sources may include eyewitnesses, third parties, other law enforcement agency personnel, social media, and other sources. Eventually, the subject of the investigation is interviewed, and information is collected directly from him or her.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The data is used to record, investigate, and resolve reports of misconduct and discipline, from the receipt of an allegation, through the investigative process, and to the final disposition/discipline. The system also provides data used for reporting to management. JICMS provides enhanced querying and sorting capabilities, which enable routine and ad hoc reports using primary data elements. These reports are generated for statistical and performance-based purposes for managing cases. Investigators gather additional background information regarding individuals associated with a case. Information gathered is documented in an ROI or if the matter was handled as an administrative inquiry, it is reported by a fact finder as an AIR.

As part of the investigative process, information from subjects, complainants, witnesses, and third parties may be used for general contact purposes, as search terms in searchable public and non-public databases for information relating to the case, and for other investigative purposes. SSNs may be used to confirm identities and trace people, assets, and transactions. The specific use of the SSN depends on the allegation under investigation.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, neither the investigators nor JICMS use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, each authorized user in CBP, ICE, NPPD, and DHS HQ is provided with a limited permission level based upon their component, office, position, and need to know.

Specific user roles are based on a determined need to know. Only appropriately cleared personnel, with a valid need to know, supervisor request, owner approval, and least-privilege access are assigned access roles to JICMS data. Below are the different user roles in JICMS:

1. Special Agent: Case agents investigate assigned cases. This role has access to the cases assigned to the agent and his case group.
2. Special Agent Supervisor: Agent supervisors can access the same cases as their subordinates and can approve ROIs created by case agents.

3. Fact Finder: This role can access only those cases assigned to it for action.
4. OIG Desk Officer: All allegation cases in JICMS are sent to OIG for first right of refusal. This role is given to OIG desk officers to review JICMS cases sent to OIG. If they choose to accept the case, they open a case in their own system.[20] The results are later uploaded by the component to the JICMS case.
5. Employee Relations Staff: This role allows employee relations staff to access assigned cases related to employee-relations functions in JICMS.
6. SETUP User: This role is given to Administrators to set up users, reset passwords.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that authorized users will use information in JICMS for unauthorized purposes.

Mitigation: This risk is mitigated because all users receive training regarding the sensitivity of the investigative records and information, as well as restrictions on disclosure through the Privacy Act, prior to gaining access to JICMS. All users gaining access to JICMS complete a background investigation and reinvestigations, as required. Qualified employees and contractors responsible for the maintenance and repair of JICMS must be granted a security clearance prior to gaining access. Departing users provide the appropriate separation notice so access to the system is revoked in a timely manner.

Privacy Risk: There is a risk that information maintained in JICMS may be accessed by users within other DHS components who do not have a need to know.

Mitigation: This risk is partially mitigated through the use of user roles. In general, all OPR users are granted access based upon their component, group affiliation, and the need to know. Users within the group affiliation are able to create and edit records, while other OPR users from the same component, outside the group affiliation, are granted read-only access. Additional user roles can be customized and expanded when there is an official need to know. For example, as the intake center for reported allegations, JIC staff have access to all case records in JICMS.

Until January 2015, ICE OPR performed the investigative functions for all CBP cases. Based upon this official need to know, ICE users were granted access to all CBP cases in JICMS. In 2015, CBP was granted the authority to conduct its own investigations, and therefore, ICE investigative services were no longer required. As a result, access to CBP cases will be restructured to limit access to those ICE users who continue to have an official need to know. The remaining CBP access roles will be rescinded.

[20] For more information about the OIG case management system, please *see* DHS/OIG/PIA-001(b) Office of Inspector General Enterprise Data System (July 10, 2015) *available at* https://www.dhs.gov/privacy.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Public Notice

The publication of this PIA, the DHS/ALL-020 Internal Affairs SORN, and the corresponding Final Rule for Privacy Act exemptions provide public notice of the collection, use, and maintenance of this information. Prior notice to individuals may not always be feasible. Notice provided to subjects of investigations could interfere with law enforcement actions and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants. The Final Rule for this system of records officially exempts the system from portions of the Privacy Act.

In addition, the OIG public website provides a link to the OIG Hotline.[21] The hotline provides: 1) notice to members of the public regarding how to report corruption and misconduct within DHS, and 2) a link to the misconduct allegation form[22] that can be completed and submitted online. Reports of misconduct also may be mailed to OIG[23] or reported to the CBP Information Center.[24]

General Notice to All DHS Employees and Contractors

DHS Management Directive 0810.1, *The Office of the Inspector General*, provides notice to all DHS employees and contractors that they are responsible for reporting suspicions of misconduct to OIG or appropriate OE offices. The specific responsibilities were discussed in the Overview section.

How CBP Provides Notice to CBP Employees and Contractors

To promote ethical behavior within CBP among employees and contractors, CBP OPR provides required annual integrity awareness training to all CBP employees and contractors. In addition, CBP OPR uses the internal CBP website to promote professional integrity in several ways:

[21] The OIG Hotline is available on the OIG homepage, *available at* https://www.oig.dhs.gov.
[22] OIG misconduct allegation form, *available at* https://www.oig.dhs.gov/hotline/hotline.php.
[23] Department of Homeland Security, 245 Murray Lane SW, Washington, D.C. 20528, Attn: Office of Inspector General, Hotline.
[24] CBP Information Center, *available at*: https://help.cbp.gov/.

- The daily "Trust Betrayed" site is designed to demonstrate CBP's commitment to combatting corruption and maintaining public trust. The site provides examples of CBP employees who betrayed the public trust and were convicted. These cases demonstrate CBP's commitment to combating corruption and maintaining vigilance and integrity within CBP.
- Guidance for reporting misconduct is provided through the link to the JIC webpage. The JIC serves as the central "clearinghouse" for receiving, processing, and tracking allegations of misconduct involving personnel and contractors employed by CBP and ICE. The following information is provided on the webpage:
    - The JIC hotline number, fax number, email address, and mailing address;
    - The OIG hotline number and online OIG Complaint/Allegation Form; and
    - The OIG mailing address.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Depending on the nature of the allegation, the subject of the investigation may not have the opportunity to consent to the use of his or her information, decline to provide information, or to opt out. Other interviewees may have the opportunity to consent or decline depending on the nature of the investigation. Investigators undergo extensive training on interviewees' rights and obligations in the context of responding to investigative inquiries. Policies and procedures are in place addressing interviewees' rights and obligations that vary depending on the type of investigation, and on whether the interviewee is a federal employee, as well as other circumstances (*e.g.*, whether the employee is a bargaining unit employee). Depending on the nature of the investigation, the interviewee may be offered the opportunity to consent and request confidentiality. Confidentiality may be extended depending on the applicable laws and regulations.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that interviewees may not realize that they may have the option to consent or decline to participate in the interview.

Mitigation: This risk is mitigated through the provision of extensive training on interviewees' rights and obligations in the context of responding to investigative inquiries to investigators. Policies and procedures are in place addressing interviewees' rights and obligations that vary depending on the type of investigation and on whether the interviewee is a federal employee.

Privacy Risk: There is a risk that the subjects of investigations may not know how to access and correct their information collected and maintained in JICMS.

Mitigation: This risk is only partially mitigated due to the law enforcement nature of the system. Although the subject of the investigation may make a request for information through the FOIA process discussed in Section 7.1, JICMS is exempted from subsection 552a(d) of the Privacy Act providing access to records and subsection 552a(e)(1) of the Privacy Act requiring correction of erroneous information. However, exceptions to these exemptions will be determined on a case-by-case basis.[25]

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

All records within JICMS are categorized by NARA as temporary. Information collected during inquiries or investigations and complaints received and reviewed by the JIC and entered into JICMS are deleted or destroyed after twenty-five (25) years or one (1) year after the subject separates from DHS, whichever is later. The JIC and CBP OPR field offices also maintain hard copy records associated with cases in accordance with the same retention rules. Information extracted from JICMS for reporting purposes also is destroyed or deleted when no longer needed for administrative, legal, audit, or other operational purposes.

During the course of adjudicating a complaint, records or information from other systems of records may become part of JICMS. JICMS may contain records or information compiled from or based on information contained in other systems of records that are exempt from certain provisions of the Privacy Act. To the extent this occurs, the same exemptions will be claimed in JICMS. Such exempt records or information are likely to include law enforcement or investigation records, law enforcement encounter records, or possibly intelligence-related information or terrorist screening records. Such records adhere to the protections described in the underlying system and are safeguarded accordingly.

5.2 Privacy Impact Analysis: Related to Retention

There is no risk to records retention. JICMS records are retained based on an approved NARA records retention schedule. NARA has categorized all JICMS records as temporary. Hard copy records collected during the inquiry or investigation of the allegation are transferred to the Federal Records Center and are kept for 25 years or 1 year after the subject leaves DHS, whichever is longer.

[25] *See* Final Rule for Privacy Act Exemptions, 74 FR 42575 (August 24, 2009).

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

JICMS does not interface with any external systems and direct access to JICMS is limited to authorized DHS employees and contractors. Contractors responsible for the installation and maintenance of JICMS software and hardware are subject to the same training and security clearance procedures as authorized DHS employees.

However, information may be shared on a case-by-case basis via email, orally during briefings and interviews, in writing, and by telephone with other government agencies, including law enforcement agencies and third parties with a need to know. The actual information shared will depend on the nature, subject, status, and other factors unique to each investigation or information request. Shared information may include: ROIs with related exhibits, statements, affidavits, records and other documents, transcripts, reports from or to other law enforcement entities, records involving the disposition of investigations, and resulting agency actions (*e.g.*, criminal prosecutions, civil proceedings, administrative action).

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The DHS/ALL-020 Internal Affairs SORN[26] permits the sharing of JICMS information in accordance with the purpose for which the information was collected and in accordance with the routine uses listed in the SORN. The purpose of JICMS is to support and protect the integrity of DHS operations; to ensure compliance with applicable laws, regulations, and policies; and to ensure the integrity of DHS employees' conduct and those acting on behalf of DHS. The SORN's routine uses define the circumstances under which information in JICMS can be shared outside DHS. A complete list of the routine uses can be found in the SORN and Final Rule referenced earlier. The following are brief examples of the information sharing permitted by these routine uses. For more extensive descriptions of these routine uses see the SORN.

- To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation (Routine Use J).
- To appropriate law enforcement authorities charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order (Routine Use G).

[26] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014).

- To appropriate agencies if the information is relevant and necessary to the agency's decision to hire, retain, or approve a security clearance of an individual (Routine Use H).
- To an authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed against DHS, its employees, contractors, offices, or components (Routine Use K).
- To union officials representing employees in investigations and personnel actions (Routine Use L).
- To management officials at various agencies who may be in a position to take disciplinary or other corrective action, and to boards and panels who may be charged with making recommendations or proposals regarding remedial action (Routine N).
- To the Office of Personnel Management (OPM) to refer an individual who has applied for federal employment in cases when there is material, intentional falsification, deception, or fraud in the initial application or examination process; or when suitability evaluation indicates a government-wide debarment should be imposed (Routine P).

6.3 Does the project place limitations on re-dissemination?

Yes, external sharing and re-dissemination of information maintained in JICMS is governed by the routine uses listed in the DHS/ALL-020 Internal Affairs SORN, discussed in Section 6.2. The sharing and re-dissemination of information by record subjects may be further restricted by the Privacy Act exemptions claimed by the Secretary of Homeland Security. Through the use of access roles, each component remains responsible for the sharing of its own data within JICMS.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Each component remains responsible for maintaining an accounting of its own disclosures. These disclosures are maintained outside of JICMS on the standard DHS 191 Accounting for Disclosures paper form. These paper forms are maintained in the associated case file in locked cabinets and in secure offices. Requests may come from Department of Justice (DOJ) and other external law enforcement agencies. Each request is separately recorded and identifies the requested information shared. Shared information is detailed in case notes and memoranda of investigation.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information in JICMS may be inappropriately shared with external recipients.

Mitigation: In general, JICMS information may be shared with recipients outside DHS when the sharing is aligned with the purpose for which the information was collected. More specifically, external sharing is governed by the DHS/ALL-020 Internal Affairs SORN, which defines the purpose for which the information was collected, and with whom and under what circumstances the information can be shared. In the case of CBP records, the *U.S. Customs and Border Protection, Office of Internal Affairs Information Sharing Standard Operating Procedure (SOP)* sets the framework for the exchange of information with third parties. This SOP requires the participation of the CBP Privacy Office prior to any ad hoc or reoccurring sharing arrangements to ensure that any third-party sharing complies with the applicable SORN.

Component users receive annual training addressing the safeguarding of information through IT security and integrity awareness, as well as privacy awareness. Non-routine sharing arrangements are reviewed by managerial staff for compliance with existing requirements, policies, and procedures prior to approval.

In addition, to ensure compliance with this information sharing process, CBP Privacy will conduct a CBP Privacy Evaluation within 12 months of the publication of this PIA. CBP Privacy will share the results of this evaluation with the DHS Privacy Office.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals may request access to or correction of any CBP record contained in JICMS, pursuant to procedures provided by the Freedom of Information Act (FOIA),[27] and access provisions of the Privacy Act of 1974 at https://www.cbp.gov/site-policy-notices/foia, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
1300 Pennsylvania Avenue, NW, Room 3.3D
Washington, D.C. 20229

Individuals seeking notification and access to records contained in JICMS, but owned by another DHS component, need to contact the FOIA office for that DHS component. Although CBP owns JICMS, each DHS customer maintains ownership of its own data, and therefore, controls the disclosure of that data. If CBP receives a FOIA or Privacy Act request for information within JICMS that belongs to a customer component, CBP will refer the FOIA or Privacy Act request to that DHS component.

[27] 5 U.S.C. § 552.

When seeking records from this system of records or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information.[28] You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury,[29] a law that permits statements to be made under penalty of perjury as a substitute for notarization. While your inquiry requires no specific form, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

As noted above, in accordance with the Privacy Act, 5 U.S.C. § 522a and the Final Rule referenced earlier in this PIA, JICMS is exempt from subsection (d) of the Privacy Act requiring information access because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose sensitive but unclassified information that could be detrimental to homeland security.

However, requests for information are evaluated by DHS on a case-by-case basis to ensure that exemptions are only taken where the request meeting the specific standards set forth in 5 U.S.C. §§ 552a(j)(2) and (k)(1), (k)(2), (k)(3), and (k)(5).

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As described in Section 7.1, individuals may file a Privacy Act request with the CBP FOIA office for a copy of records they believe to be in JICMS containing information about them. The

[28] 6 CFR Part 5.
[29] 28 U.S.C. § 1746.

requests may be subject to applicable exemptions. Individuals then may request amendment of inaccurate records in JICMS.

JICMS is exempt from subsections 552a(e)(1) and (d)(2) of the Privacy Act requiring correction of erroneous information. However, requests for redress are evaluated by DHS on a case-by-case basis. During the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity.

7.3 How does the project notify individuals about the procedures for correcting their information?

Through the publication of this PIA, individuals seeking notification of and access to any record contained in JICMS are informed that they may submit a request through the procedures in Sections 7.1 and 7.2, above. Individuals also receive notice via the governing SORN described in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to access, correct, and amend records about themselves given the law enforcement and investigatory nature of JICMS.

Mitigation: This risk cannot be fully mitigated. Given the nature of internal investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity.

However, this risk is partially mitigated because by policy and pursuant to published SORNs, all requests for access, correction, and amendment of Privacy Act-covered records are evaluated by DHS on a case-by-case basis, regardless of exemption.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Access to JICMS is controlled via user roles and auditing. Access to each case is restricted to those with a need to know. Individual cases have access controls that restrict access and restrict edit capabilities per case. In most situations, access to a case is limited to the specified case agent,

case officer, and case supervisor who are assigned to work the given case. In addition, JICMS automatically generates notifications if an individual has not logged on in the last 45 days, prompting a review of that individual's need for access.

User actions are audited in JICMS. The audit trail tracks the modification made, the user that made the modification, and the date/time the modification was made. The JICMS administrator can view audit trails when needed, and the system Information System Security Officer (ISSO) routinely reviews audit trails. In addition, data can only be accessed using the DHS network with a Personal Identity Verification (PIV) card and single sign-on to access the JICMS web-based interface.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

In general, the CBP Office of Information and Technology IT Training Branch requires all users to complete the Privacy Awareness Computer Based Training course annually. Failure to complete the course results in the removal of access to the system.

More specifically, JICMS users receive formal JICMS training and user manuals that address the appropriate procedures for handling the highly sensitive information maintained in JICMS.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

As a preliminary requirement, the requestor must be an OPR employee (or serve an equivalent function in another component), who has successfully completed a background investigation. Upon meeting this preliminary criteria, the requestor fills out a user request form and has it approved by his or her supervisor. Then the form is reviewed by the component liaison and submitted to the JICMS Help Desk for processing. The Help Desk reviews the form for completeness and then forwards the form to the JICMS Information System Security Officer (ISSO) for review and approval. Upon completion of the review, the ISSO either emails or faxes an approval or rejection of the application back to Help Desk. When the Help Desk receives the approval, the user account is created and activated, and an email notification is sent to the requestor. The forms are stored in a secure location in the ICE OPR headquarters office.

User identification and authentication prevents unauthorized people (or unauthorized processes) from entering JICMS. All users of the JICMS systems must use their PIV card and single sign-on to access the system.

JICMS applies identification and authentication rules and authenticates the user. Upon logging into the web application, the user's credentials are passed to the database for

authentication. Users are granted access to JICMS based on profiles assigned within the application.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Information sharing is done on a case-by-case basis via email, orally during briefings and interviews, in writing, and by telephone with other government agencies, law enforcement agencies, and third parties with a need to know, and follows the requirements described in Section 6.0 of this PIA. The actual information shared will depend on the nature, subject, status, and other factors unique to each investigation or information request. Shared information may include: ROIs with related exhibits, statements, affidavits, records and other documents, transcripts, reports from or to other law enforcement entities, records involving the disposition of investigations, and resulting agency actions (*e.g.*, criminal prosecutions, civil proceedings, administrative action).

Responsible Officials

William K. Townsend
Assistant Special Agent in Charge, Investigative Operations Division
Office of Professional Responsibility
U.S. Customs and Border Protection
Department of Homeland Security

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A: Data Sources

Human Resources Business Engine (HRBE)

JICMS shares basic employee information and minimal case data with, and imports data from HRBE. Presently, there exists a bi-directional interface from JICMS to the CBP LER and ICE ELR module in HRBE. The data shared between JICMS and HRBE is as follows:

Outbound Fields to HRBE:

1. Allegations
2. Case Number
3. Case Officer ID
4. Case Type
5. Fiscal Year
6. Has Priors
7. Incident Date
8. LER Received Date
9. SSN
10. Subject Office
11. Team

Inbound Fields from HRBE:

1. Incident Number
2. The Case Is (Case Workflow Process Stage)
3. Status
4. Decision Action 1
5. Decision Action 1 Days
6. Decision Action 2
7. Deciding Official
8. Decision Issued
9. User Name

Personnel Information Originating from USDA NFC (PB2 Database) Inbound (Employee interface to update employee information in JICMS)

1. Last Name
2. First Name
3. Middle Name
4. SSN
5. City
6. State
7. Organization Code
8. Title
9. Grade
10. Position Series
11. DOB
12. Hash ID
13. User Name
14. Oracle Employee ID
15. Oracle Party ID
16. Oracle Resource ID
17. User Creation
18. Office Code
19. Approval Code
20. Profile Code
21. Gender
22. Hire Date
23. Country
24. Email
25. Status Code
26. Agency Code

27. Duty Station

28. Separation Date